(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 812 948 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.04.2025 Bulletin 2025/18

(21) Application number: **19878392.0**

(22) Date of filing: **16.01.2019**

(51) International Patent Classification (IPC):
G06F 21/85 *(2013.01)* ***G06F 21/56*** *(2013.01)*
G06F 21/44 *(2013.01)*

(52) Cooperative Patent Classification (CPC):
G06F 21/85; G06F 21/44; G06F 21/567;
G06F 2221/2129

(86) International application number:
PCT/CN2019/072029

(87) International publication number:
WO 2020/087781 (07.05.2020 Gazette 2020/19)

(54) EXTERNAL CONNECTION TYPE TERMINAL PROTECTION DEVICE AND PROTECTION SYSTEM

ANSCHLUSSSCHUTZVORRICHTUNG VOM EXTERNEN VERBINDUNGSTYP UND SCHUTZSYSTEM

DISPOSITIF DE PROTECTION DE TERMINAL DE TYPE À CONNEXION EXTERNE ET SYSTÈME DE PROTECTION

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **29.10.2018 CN 201811264781**

(43) Date of publication of application:
28.04.2021 Bulletin 2021/17

(73) Proprietor: **Beijing Beyondinfo Technology Co., Ltd.**
Beijing 100020 (CN)

(72) Inventors:
- **DU, Hua**
  Beijing 100020 (CN)
- **AI, Wei**
  Beijing 100020 (CN)
- **CAI, Zhenhe**
  Beijing 100020 (CN)
- **ZHANG, Hao**
  Beijing 100020 (CN)

(74) Representative: **Zaboliene, Reda**
Metida
Business center Vertas
Gyneju str. 16
01109 Vilnius (LT)

(56) References cited:
CN-A- 103 532 978
CN-A- 103 532 980
CN-A- 108 537 072
CN-U- 203 618 018
CN-U- 203 618 020
FR-A1- 2 949 888
US-A1- 2006 072 241
US-A1- 2015 365 237
US-A1- 2018 137 278
US-B1- 7 877 788

Note: Within nine months of the publication of the mention of the grant of the European patent in the European Patent Bulletin, any person may give notice to the European Patent Office of opposition to that patent, in accordance with the Implementing Regulations. Notice of opposition shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

EP 3 812 948 B1

Description

TECHNICAL FIELD

[0001] The present invention relates to the technical field of computer security, and more particularly to an external terminal protection device and a protection system.

BACKGROUND

[0002] In recent years, the computer and information technology develops rapidly, thereby greatly promoting the popularization of networks. While people are enjoying the convenience brought by the computer and information technology, the technology also brings new threats to the security of data in computers used by people in production/life, such as the following common threats: unauthorized access, personating a valid user, destroying data integrity, interfering normal system operation, utilizing a network to spread virus, man-in-the-middle eavesdrop and the like.

[0003] The technical means to solve the problem of intranet security are varied, for example, installing and using a network security product in a host such as a firewall, an anti-virus and intrusion detection system and the like. However, even if the above measures are taken, various network security events still occur frequently. According to statistics, 70% of computer crimes occur because an internal person illegally uses a key resource such as the host and the like, and the threats really coming from the outside are only 30%. The internal person lacks security awareness when using the host. The behaviors of the internal person at the back end of the firewall, such as nonstandard access of various external devices, system mis-operation or intentional damage, would result in dreadful influence on or bring heavy loss to organizations, enterprises and institutions.

[0004] Furthermore, for certain special devices, such as a host equipped with a special software control, and a device at an engineer station/staff station in certain industrial fields, generally no security protection software adapted to the system of the host/device is sold on the market because the system is special or because the installation of security software is easy to cause the compatibility problem of the original software of the host, and even influence performance. In addition, the host of the engineer station/staff station basically does not upgrade an operating system after the host gets on line. Even after security software is installed, the host generally does not update an anti-malicious code software version or a malicious code library in time, and thus cannot play an overall security protection role.

[0005] US2015/365237A1 discloses a USB gateway connected to a plurality of host computers having a USB device port connect to a peripheral device; and a security circuitry. The security circuitry comprises: a pre-qualification microcontroller; a mode select switch connected to the peripheral device port and selectively connecting it to one of : the pre-qualification microcontroller; or to a host selector switch that switches among the plurality of connected host computers. An enumeration and reset detector is connected to the USB peripheral device port to monitor that port and casing the mode select switch to switch back to the pre-qualification microcontroller when the peripheral device is disconnected or reset. The pre-qualification microcontroller is capable of enumerating a connected peripheral device and controlling the gateway according to a table containing lists of : device qualifications, indication of which device can connect to each host, and direction of data flow between host and device. The table of peripheral device qualifications may be field re-programmed.

[0006] US7877788B1 discloses a method and apparatus for controlling connectivity comprising a connectivity control element coupled between an interface connector and an interface circuit, and an interface controller, coupled to the connectivity control element, for authenticating a peripheral device and controlling connectivity between the interface connector and the interface circuit based upon authentication of the peripheral device.

[0007] US20180137278A1 discloses a method of enhancing security of at least one of a host computing device and a peripheral device coupled to the host computing device through a communication interface. Data is transparently received from the peripheral device or the host computing device, and the received data is stored. The stored data is analyzed to detect a circumstance associated with a security risk. If such a circumstance is not detected, then the data is transparently forwarded to the other of the peripheral device or the host. However, if a circumstance associated with a security risk is detected, then a security process, defined by a rule, is performed. Related apparatus are provided, as well as other methods and apparatus.

[0008] FR2949888A1 discloses an apparatus for protecting against the malware connector comprising a port enabling it to be connected via a first interface to an electronic equipment called host equipment, at least one port receptacle for enabling at least one peripheral device to connect to the protection device via a second interface, said protection device being characterized in that it comprises an operating system for simulating a host equipment, said device also being able to be perceived by the peripheral device as a host apparatus.

SUMMARY

[0009] On the basis of the existing status, the present invention provides an external terminal protection device and a protection system as defined in the appended claims to solve the above problem. In the present invention, various interfaces of a protected host are taken over, and the use of a USB interface or a serial interface device of the protected host must be completed via the external terminal protection device, such that the USB interface or

serial interface of the protected host can be protected without installing security protection software on the protected host.

[0010] In a first aspect, the present application provides an external terminal protection device, including:

an interface control module, used for providing one or more internal interfaces and one or more external interfaces, the internal interfaces being connected to corresponding interfaces of a protected host, and the external interfaces being configured to access one or more external devices; and

a system control module, used for connecting the interface control module via a bus, and controlling security authentication of the external device accessed to the one or more external interfaces on the interface control module, so as to determine whether the external device is a licensed access device.

[0011] Optionally, when the external interface of the interface control module accesses the external device, the interface control module notifies, via the bus, the system control module that the system control module first performs a security authentication operation on the external device.

[0012] Optionally, if the external device does not pass the security authentication, then the external device is set to be an unlicensed access device, and a physical circuit between the external device and the protected host is kept in a disconnected state; and/or

if the external device passes the security authentication, then the external device is determined to be a licensed access device, and the physical circuit between the external device and the protected host is switched on.

[0013] Optionally, the interface control module monitors in real time a connection state of the external interface accessing the external device, and automatically disconnects the physically connected circuit when the external device determined to be a licensed access device is unplugged from the external interface.

[0014] Optionally, when the external device is re-accessed after being unplugged from the external interface, the system control module re-performs the security authentication operation on the external device.

[0015] Optionally, the interface control module monitors in real time a connection state of the internal interface connected to the corresponding interface of the protected host;

when the connection state is abnormal, the disconnection of a circuit between the interface control module and the protected host is automatically triggered.

[0016] Optionally, when the connection state is abnormal, automatically triggering the disconnection of the circuit between the interface control module and the protected host further includes:

capturing a current/voltage change of the internal interface via a monitoring circuit, determining that the connection state is abnormal, and triggering an alarm indication signal.

[0017] Optionally, after the disconnection of the circuit between the interface control module and the protected host is automatically triggered, the connection state restores from abnormality to normality, and the circuit between the interface control module and the protected host is still kept in the disconnected state.

[0018] Optionally, the system control module controls, on the basis of a preset security policy, the security authentication of the external device accessed to the one or more external interfaces on the interface control module.

[0019] Optionally, the external terminal protection device further includes:

an internal memory, used for storing data exchanged between the interfaces.

[0020] Optionally, the interface control module adopts a current and voltage limited circuit to prevent the external terminal protection device from being damaged when the external interface accesses a strong discharging device.

[0021] Optionally, one or more of the internal interfaces and the external interfaces are USB interfaces.

[0022] Optionally, one or more of the internal interfaces and the external interfaces are serial interfaces.

[0023] In a second aspect, the present application provides a protection system, including:

one or more external devices,

a protected host, and

the external terminal protection device as described above,

wherein the external terminal protection device is externally connected to the protected host, such that the one or more external devices perform interface communication with the protected host via the external terminal protection device.

[0024] The technical solution of the present invention at least has the following one or more technical effects: the present invention takes over various data interfaces of the protected host, so as to ensure that the data communications of the interfaces of the protected host are all completed via the external device; the present invention can protect the security of the protected host without installing security protection software on the protected host, thereby greatly reducing system security risks, and comprehensively solving potential security hazards that may be generated by the interfaces.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025]

Fig. 1 is a schematic view of an application scenario of a protection system based on an external terminal protection device according to a first embodiment of

the present invention;

Fig. 2 is a schematic view of an internal structure of the external terminal protection device according to the first embodiment of the present invention;

Fig. 3 is a connection view of the external terminal protection device according to a second embodiment of the present invention; and

Fig. 4 is a network deployment view of the protection system based on the external terminal protection device according to a third embodiment of the present invention.

DETAILED DESCRIPTION

[0026] The exemplary embodiments of the present disclosure will be described in detail hereafter with reference to the drawings. Although the exemplary embodiments of the present invention are shown in the drawings, it should be understood that the present invention can be realized in various forms and shall not be limited to the embodiments elaborated herein. On the contrary, the embodiments are provided such that the present invention can be understood more thoroughly and the scope of the present invention can be completely conveyed to a person skilled in the art.

[0027] The term "and/or" herein only describes an association relationship between associated objects, and can denote three relationships, for example, "A and/or B" can denote A, both A and B, and B. In addition, the character "/" herein generally denote that the former and latter associated objects are in an "or" relationship.

[0028] The external terminal protection device provided by the present invention includes an interface control module and a system control module. The interface control module provides an internal interface and an external interface, the internal interface being connected to a corresponding interface of a protected host, and the external interfaces being configured to access one or more external devices. The system control module is used for electrically connecting the interface control module, and controlling security authentication of the external device accessed to the one or more external interfaces on the interface control module. Therefore, the present invention provides a hardware form terminal protection device, and can protect the security of the protected host without installing security protection software on the protected host, thereby greatly reducing system security risks, and comprehensively solving potential security hazards that may be generated by the interfaces.

[0029] It should be noted that the term "module" in the present invention is a hardware module consisting of tangible electronic elements such as a circuit, a data processing apparatus, a memory, a buffer and the like. In the present invention, the interface control module and the system control module can be a physically or functionally independent element combination, and can also be a physically or functionally integrated integral element combination. For example, as an embodiment, the interface control module consists of an interface control board, and the system control module consists of a system control board; the interface control board and the system control board are both circuit boards integrated with electronic elements, and are connected via a bus. In other embodiments, the interface control module and the system control module can also be integrated on one circuit board. Therefore, the key of the present invention is a control relationship between the interface control module and the system control module, but not limited to the space or physical connection combination modes of the electronic elements forming the modules.

[0030] According to the present invention, when the external interface of the interface control module accesses the external device, the interface control module notifies the system control module that the system control module performs a security authentication operation on the external device. If the external device does not pass the security authentication, then the external device is set to be an unlicensed access device, and a physical circuit between the external device and the protected host is kept in a disconnected state; and/or if the external device passes the security authentication, then the external device is determined to be a licensed access device, and the physical circuit between the external device and the protected host is switched on. Therefore, the present invention realizes physically isolated security authentication of the external device, thereby improving the security performance of the protection system.

[0031] As a specific embodiment, the interface control module monitors in real time a connection state of the external interface accessing the external device, and automatically disconnects the physically connected circuit when the external device determined to be a licensed access device is unplugged from the external interface. Therefore, the present invention can prevent an unlicensed access device from accessing by utilizing the connection of a licensed access device.

[0032] Preferably, when the external device is re-accessed after being unplugged from the external interface, the system control module re-performs the security authentication operation on the external device. Therefore, the present invention can prevent the attack behavior utilizing the same external device.

Embodiment

[0033] Fig. 1 shows an application scenario of the protection system according to a first embodiment of the present invention.

[0034] As shown in Fig. 1, the external terminal protection device is externally connected to the protected host via interface connecting wires; the interfaces (USB interfaces UC1, UC2, a COM interface CC0, a network interface EC0) on the protected host to be protected are connected to the internal interfaces of the external terminal protection device via various types of connecting wires, for example, the interfaces UC1 and UC2 of the

protected host are respectively connected to internal USB interfaces UA4 and UA3 of the external terminal protection device, the serial interface CC0 is connected to an internal serial interface CA2, and the network interface EC0 is connected to an internal network interface EA2. Various external devices (a U disk, an optical disk driver, a serial interface connection device and the like) all access the external terminal protection device, and can communicate data with the protected host only via the external terminal protection device, for example, the U disk accesses an external interface UA1 of the external terminal protection device, the USB optical disk driver accesses an external interface UA2, and the serial interface connection device accesses an external interface CA1. The external devices such as a U disk, a USB optical disk driver, and a serial interface connection device which need to communicate data with the protected host cannot directly access the protected host, but must access corresponding external interfaces of the external terminal protection device to perform forwarding communication.

[0035] Fig. 2 is a schematic view of an internal structure of the external terminal protection device according to the above embodiment of the present invention.

[0036] In the embodiment, the external terminal protection device mainly consists of an interface control board A and a system control board B, wherein the system control board B is connected to the interface control board A via a control connecting wire (for example, a bus), and is used to control different operating modes of interfaces on the interface control board A, such as a USB interface, a serial interface, and a network interface, so as to realize the function of performing security control on the access of various external devices. The system control board A can control the operating mode of each interface; the operating mode includes: available, not available, protocol filtration, flow mirroring, flow auditing and the like. However, the present invention is not limited to specific operating mode control types. The system control board B can be connected to the interface control board A via an interface I2C or SPI. However, the present invention is not limited to specific control connection interfaces.

[0037] The external terminal protection device further includes a hardware memory D which acts as an internal memory of the terminal protection device and is used for storing data exchanged between the interfaces; further, the internal memory can further store a preset security policy; and the system control board B performs security authentication on different types of interfaces or interfaces with different serial numbers on the interface control module by reading the preset security policy stored in the internal memory.

[0038] In the embodiment, the security functions realized by the external terminal protection device include but not limited to: an administrator presets a permission and a security policy for the external terminal protection device; the security policy includes but not limited to: a data import enabling policy (for example, a USB interface), a data export enabling policy (for example, a USB interface), a USB access device limitation policy (for example, a USB device based vendor ID, namely a supplier identification code, and/or a product ID, namely a product identification code), a data import anti-virus policy, a policy for controlling data export black and white lists, a data export format control policy, a serial interface access enabling policy, a USB interface plug-in protection policy, a network communication audit enabling policy, a firewall function enabling policy, a policy for serial interface command black and white lists and the like.

[0039] In a preferred embodiment, the security policy includes: after the administrator sets the security policies, the relevant security policies will be executed by the external terminal protection device one by one. In a preferred embodiment, the security policy includes: the administrator further controls whether the external terminal protection device enters a monitoring protection mode, in which mode the connection with the protected host will be monitored and an alarm will be sent in case of abnormality.

[0040] In a preferred embodiment, the security policy includes: when an abnormality alarm or an interface access situation needs to be recorded for the administrator to query subsequently, the internal memory D is further used to record alarm information or interface access log information.

[0041] **In** a preferred embodiment, the interface protection of the external terminal protection device can further include electrical security protection, and abnormality situation protection in use, and includes but not limited to: trying to forcedly bypass the external terminal protection device, and trying to access an illegal USB device after using a legal USB device to pass a security authentication.

[0042] **In** a preferred embodiment, the electrical security protection of the external terminal protection device refers to the external terminal protection device can effectively prevent, via the external interface such as a USB, the protected host from physical hardware damage, and can prevent the behavior of damaging the protected host by means of a strong discharging device such as a USB bomb.

[0043] In order to realize the object, a preferred embodiment of the present invention makes targeted designs for the electrical security protection from two aspects:

1) the interface adopts a current and voltage limited design

In the solution, the electrical security protection of the terminal protection device refers to that the device adopts a hardware design to prevent the damage of the strong discharging device, and introduces a current and voltage limited circuit to prevent current and voltage from too heavy, so as to construct a first protection system;

2) an external device connection mechanism based

on physical switch switching

[0044] The external terminal protection device introduces a hardware switching logic, and further improves the electrical security protection function. By taking a USB external device as an example, when a U disk device or other USB device is plugged in the terminal protection device, first necessary security authentication must be performed, and only the licensed device is allowed to perform the next operation; before passing the security authentication, the plugged USB device cannot be connected to the protected host. In other words, before the plugged external device passes the security authentication, no connected circuit is provided between the external device and the protected host. Therefore, even if the current and voltage limited design in the first protection layer does not play a due role, current and voltage surges caused by the plugged USB device would not influence the security of the protected host.

[0045] As an optional embodiment, the external terminal protection device has an interface abnormality situation protection function in use; the function mainly prevents from situations that a malicious user disconnects the circuit between the external terminal protection device and the protected host, tries to bypass the external terminal protection device and directly access the protected host, or uses a legal USB device to pass the security authentication and then replaces the legal device with an illegal USB device.

[0046] A preferred embodiment of the present invention makes targeted designs for the abnormality situation protection in use:

1) interface connection locking, for example, USB connection locking

[0047] A conventional interface is generally locked in a mechanical manner, namely via a special interface, for example, a special wide interface U disk or a special network interface used in the secret involved industry, so as to prevent misuse or prevent another person from plugging and unplugging the interface. Such interfaces have the defect of poor generality, and a device interface needs to be reconstructed to satisfy a mechanical connection requirement. Such interfaces are generally only suitable for mandatory management devices in special industries, are poor in implementation, and are easy to lead to device maintenance disputes.

[0048] The external terminal protection device provided by a preferred embodiment of the present invention has an interface locking function which is realized through an analog signal sampling and analog-to-digital conversion signal acquisition technology; when a specific interface of the external terminal protection device A is connected to a specific interface of the protected host B, the interface control board in the external terminal protection device monitors in real time the connection state of the internal specific interface connected to the protected host B; and when the connection state is abnormal, the disconnection of the circuit between the interface control board and the protected host is automatically triggered. Further, a current/voltage change of the internal interface is captured via a monitoring circuit; and when the connection state is determined to be abnormal, an alarm indication signal is triggered. Still further, after the disconnection of the circuit between the interface control board and the protected host is automatically triggered, the connection state restores from abnormality to normality, and the circuit between the interface control board and the protected host is still kept in the disconnected state. Taking a USB interface connection between the two as an example, the external terminal protection device A monitors in real time current and voltage situation of the interface connected to the protected host B, so as to obtain the situation of the connecting wire between the device A and the host B. When a malicious user unplugs the connecting wire between the device A and the host B, the monitoring circuit captures in time current and voltage changes, triggers an acousto-optic alarm, and triggers a disconnection operation; even if the user plugs the connecting wire back, the connection between A and B would not be automatically restored, instead, the restoration of the connection needs manual configuration of a user with an administrator permission.

2) External device plug and unplug monitoring

[0049] The external terminal protection device provided by the technical solution of the present invention has an external device plug and unplug monitoring function; the function refers to: the interface control board monitors in real time a connection state of the external interface accessing the external device, and automatically disconnects the physically connected circuit when the external device determined to be a licensed access device is unplugged from the external interface; further, when the external device is re-accessed after being unplugged from the external interface, the system control board 2 re-performs the security authentication operation on the external device. As an embodiment, when the user is authorized to perform data import and export operations, the external terminal protection device A effectively monitors the plugged external device (for example, a USB device) by monitoring the interface, and prevents the behavior that the user uses a legal device to pass security authentication and then unplugs the legal device and plugs an illegal device. Once the user unplugs the device, the system will automatically restore to an unauthorized disconnected state, so as to ensure device connection security to the most extent.

[0050] The terminal protection device provided in the solution has a plug-unplug monitoring and abnormality disconnection function; the function is realized by means of connection switching under the control of specific hardware, but not software; the design drawing of the

hardware is as shown in Fig. 3.

[0051] Fig. 3 shows another embodiment of the present invention. The external terminal protection device of the embodiment has an interface control function, and adopts the solution that the hardware is connected/disconnected by switching on/off a hardware isolating switch on the basis of FPGA/single chip microcomputer control, so as to control the access switching of the external device.

[0052] Taking a USB control function as an example, the external terminal protection device of the embodiment includes an interface control board, an ARM/x86 based system control board, and an internal USB storage device, wherein the interface control board includes an AD acquisition module and a switching chip.

[0053] The interfaces of the interface control board are connected as shown in Fig. 3. UA1 and UB1, UA2 and UB2, UA3 and UB3, UA2 and UA4, UB1 and UB3 are switched via switches. The AD acquisition module detects the state of each interface; and the switching chip is configured to communicate network interface data between the protected host, the external terminal protection device, and a remote control center.

[0054] The hardware supports two control modes which respectively correspond to two use functions of the USB device: USB data import and export, and USB device direct-connection:

1) USB data import and export control logic:

[0055] For the data import and export control logic of the external terminal protection device of the embodiment, the hardware connection situation is as follows: a USB connecting wire of the protected host is plugged in the internal interfaces UA3 and UA4; UB1 and UB2 access a USB interface of the system control board; a U disk to be accessed or a mobile storage medium is plugged in the external interface UA1; a USB optical disk driver device is plugged in UA2; and UB3 accesses the internal USB storage. In this way, the external terminal protection device takes over all the data interfaces of the protected host, such that the data communications using the interfaces of the protected host are all completed via the external terminal protection device.

[0056] Preferably, the protection system further includes a control center for remotely controlling the external terminal protection device, wherein the remote control center is connected to the network interface EA2 of the external terminal protection device via a network, and remotely controls the external terminal protection device, so as to achieve the object of protecting the security of the protected host without installing security protection software on the protected host.

2) USB device direct-connection control logic:

[0057] The embodiment provides a solution for some non-storage USB devices to be directly accessed, such as a USB optical disk driver, an encryption lock and the like; the device direct-connection control logic controls, via the system control board, the hardware control logic of the interface control board to realize the control of the data flow of the USB device; the hardware connection situation is as follows: the internal USB interface UA4 of the interface control board in the terminal protection device is connected to the USB interface UC1 of the protected host; the forwarding interface UB2 accesses the USB interface of the system control board; the external device (for example, the USB optical disk driver) to be directly connected to the protected host B is plugged in the external USB interface UA2; and the interface control board is connected to the system control board via a control line.

[0058] Preferably, the terminal protection device adopts the following method to control USB device direct-connection: when the external device (for example, a USB optical disk driver) to be directly connected to the protected host B is plugged in the external USB interface UA2 of the terminal protection device, the interface control board notifies the system control board via the control line, and the system control board controls the hardware control logic of the interface control board to switch on the physical circuit between the interface UA2 and the forwarding interface UB2, such that the USB optical disk driver plugged in the interface UA2 is connected to the USB interface of the system control board. In the meanwhile, the hardware control logic keeps the physical circuit between the interface UA2 and the internal interface UA4 connected to the protected host in the disconnected state.

[0059] The system control board performs security authentication on the USB optical disk driver on the interface UA2, and determines whether the external device is a licensed access device; after the USB optical disk driver is determined to be a licensed access device, the hardware control logic switches on the physical circuit between the external interface UA2 and the internal interface UA4, so as to connect the USB optical disk driver plugged in the interface UA2 to the protected host.

[0060] When the system control board monitors that the connection states of one or more interfaces change, the hardware control logic automatically disconnects the physical circuits between the interfaces and other interfaces. For example, when the external device plugged in the interface UA2 accesses the interface UA4, the system control board monitors in real time the connection state of the external device plugged in the interface UA2 of the interface control board, and automatically disconnects the circuit once the external device is detected to be unplugged from the interface.

[0061] Fig. 4 is a network deployment embodiment of the protection system based on the external terminal protection device according to the present invention. The protection system includes one or more external devices, a protected host, and an external terminal protection device, wherein the external terminal protection

device is externally connected to the protected host, such that the one or more external devices perform interface communication with the protected host via the external terminal protection device. Herein, the external terminal protection device is as described above, and will not be repeated here.

[0062] Further, the protection system further includes a control center for remotely controlling the external terminal protection device, wherein the control center consists of a server, a management workstation, and other nodes, and is connected to a network interface EA1 of the external terminal protection device via a network switching node.

[0063] In the description provided herein, a large number of specific details are described. However, it can be understood that the embodiments of the present invention can be implemented without the specific details. In some embodiments, commonly known methods, structures and technologies are not described in detail, so as not to obscure understanding of the description. Similarly, it should be understood that in order to simplify the present invention and help people understand one or more aspects of the present invention, in the description of the above exemplary embodiments of the present invention, the features of the present invention sometimes are together grouped into a single embodiment, a figure, or the descriptions thereof. However, the disclosed method should not be interpreted to reflect the following intention: the claimed invention claims more features than the features explicitly stated in each claim. Therefore, claims that follow a specific embodiment are hereby expressly incorporated into the specific embodiment, with each claim standing on its own as a separate embodiment of the disclosure.

[0064] Those skilled in the art may understand that the modules in the device in the embodiment may be adaptively changed and set in one or more devices different from the present embodiment. The modules or units or components in the embodiments may be combined into one module or unit or assembly, and furthermore, these may be divided into a plurality of submodules or subunits or sub-assemblies. Except that at least some of such features and/or processes or units are mutually exclusive, all features disclosed in this specification (including the accompanying claims, abstract, and drawings) and all processes or units of any method or device so disclosed may be combined in any combination. Unless otherwise stated, the features disclosed in the specification (including the accompanying claims, abstract, and the drawings) can be replaced with alternative features providing the same, equivalent or similar objects.

[0065] In addition, those skilled in the art can understand that although some embodiments described herein include certain features included in other embodiments and not others, combinations of features of different embodiments are meant to be within the scope of the disclosure and form different embodiments. For example, in the claims, any one of the claimed embodiments can be used in the form of any combination.

[0066] The component embodiment of the present invention can be realized as hardware, or a software module operating on one or more processors, or a combination thereof. A person skilled in the art should understand that in practice, a microprocessor or a digital signal processor (DSP) can be used to realize some or the entire functions of some or the entire components of a photographing and recording apparatus, a computing device, and a computer readable storage medium according to the literal contents of the embodiments of the present invention. The present invention can also be realized as a device or an apparatus program (for example, a computer program and a computer program product) for executing a part of or the entire method described herein. Such program realizing the present invention can be stored in a computer readable medium, or can adopt the form having one or more signals. Such signals can be downloaded from an Internet website, or provided on a carrier signal, or provided in any other form.

Claims

1. An external terminal protection device, comprising:

an interface control module, used for providing, a first external interface (UA1), a second external interface (UA2), a first forwarding interface (UB1), a second forwarding interface (UB2), an internal storage interface (UB3), a first internal interface (UA3) and a second internal interface (UA4), the first internal interface (UA3) and the second internal interface (UA4) being connected to corresponding interfaces of a protected host, the first external interface (UA1) being configured to be accessed by a storage type external device, and the second external interface (UA2) being configured to be accessed by a non-storage type external device;

a system control module, comprising a USB interface, the first forwarding interface (UB1) and the second forwarding interface (UB2) accessing the USB interface, furthermore, the system control module being connected to the interface control module via a control line, and controlling security authentication of any of the external devices accessed to the one or more external interfaces on the interface control module, so as to determine whether the external device is a licensed external device, and no connection being provided between the external device and the protected host before the plugged external device passes the security authentication; and

an internal memory used for storing data exchanged between the interfaces,

wherein

when one of the external interfaces of the interface control module accesses an external device, the interface control module notifies the system control module that the system control module performs a security authentication operation on the external device;
when a non-storage type external device is plugged in the second external interface (UA2), the interface control module notifies the system control module via the control line, and the system control module controls hardware control logic of the interface control module to switch on a physical circuit between the second external interface (UA2) and the second forwarding interface (UB2), such that the non-storage type external device is connected to the USB interface of the system control module, during this time, the hardware control logic keeps a physical circuit between the second external interface (UA2) and the second internal interface (UA4) connected to the protected host in a disconnected state;
if the external device does not pass the security authentication, then the external device is set to be an unlicensed access device, and a circuit between the external device and the protected host is kept in a physically disconnected state;
if the external device is a non-storage type external device and passes the security authentication, then the external device is determined to be a licensed access device, and a physical circuit between the second external interface (UA2) and the second internal interface (UA4) of the interface control module is switched on, so as to switch on the physical circuit between the non-storage type external device and the protected host; and
if the external device is a storage type external device and passes the security authentication, then the internal storage interface (UB3) accesses the internal memory, the connection state between the first external interface (UA1) for accessing a storage type external device and the first forwarding interface (UB1) are switched on by a switch of interface control module, the connection state between the first forwarding interface (UB1) and the internal storage interface (UB3) are switched on by a switch of interface control module, and the connection state between the internal storage interface (UB3) of the first internal interface (UA3) of the interface control module are switched on by a switch of interface control module; and
the interface control module monitors in real time a connection state of the external interface accessed by the external device, and automatically disconnects the physically connected circuit when the external device determined to be a licensed access device is unplugged from the external interface.

2. The external terminal protection device according to claim 1, wherein when the external device is re-accessed after being unplugged from the external interface, the system control module re-performs the security authentication operation on the external device.

3. The external terminal protection device according to claim **1,** wherein

the interface control module monitors in real time a connection state of all of the internal interfaces connected to the corresponding interface of the protected host;
when the connection state is abnormal, the disconnection of a circuit between the interface control module and the protected host is automatically triggered.

4. The external terminal protection device according to claim 3, wherein
when the connection state is abnormal, automatically triggering the disconnection of the circuit between the interface control module and the protected host further comprises:
capturing a current/voltage change of the any one of internal interfaces via a monitoring circuit, determining that the connection state is abnormal, and triggering an alarm indication signal.

5. The external terminal protection device according to claim 4, wherein
after the disconnection of the circuit between the interface control module and the protected host is automatically triggered, the connection state restores from abnormality to normality, and the circuit between the interface control module and the protected host is still kept in the disconnected state.

6. The external terminal protection device according to claim 1, wherein
the system control module controls, on the basis of a preset security policy, the security authentication of the external device accessed to the one or more external interfaces on the interface control module.

7. The external terminal protection device according to claim 1, wherein
the interface control module comprises a current and voltage limited circuit for preventing the external terminal protection device from being damaged when the external interface accesses a strong discharging device.

8. The external terminal protection device according to

claim 1, wherein
one or more of the internal interfaces and the external interfaces are USB interfaces.

9. A protection system, comprising:

one or more external devices,
a protected host, and
the external terminal protection device as claimed in any one of claims 1-8,
wherein the external terminal protection device is externally connected to the protected host, such that the one or more external devices perform interface communication with the protected host via the external terminal protection device.

Patentansprüche

1. Eine Anschlussschutzvorrichtung vom externen Verbindungstyp, umfassend:

ein Schnittstellensteuerungsmodul, das verwendet wird, um eine erste externe Schnittstelle (UA1), eine zweite externe Schnittstelle (UA2), eine erste Weiterleitungsschnittstelle (UB1), eine zweite Weiterleitungsschnittstelle (UB2), eine interne Speicherschnittstelle (UB3), eine erste interne Schnittstelle (UA3) und eine zweite interne Schnittstelle (UA4) bereitzustellen, wobei die erste interne Schnittstelle (UA3) und die zweite interne Schnittstelle (UA4) mit entsprechenden Schnittstellen eines geschützten Hosts verbunden sind, die erste externe Schnittstelle (UA1) so konfiguriert ist, dass sie von einem externen Speichertyp-Gerät zugegriffen wird, und die zweite externe Schnittstelle (UA2) so konfiguriert ist, dass sie von einem nicht speichernden externen Gerät zugegriffen wird;
ein Systemsteuerungsmodul, das eine USB-Schnittstelle umfasst, wobei die erste Weiterleitungsschnittstelle (UB1) und die zweite Weiterleitungsschnittstelle (UB2) auf die USB-Schnittstelle zugreifen, weiterhin ist das Systemsteuerungsmodul über eine Steuerleitung mit dem Schnittstellensteuerungsmodul verbunden und steuert die Sicherheitsauthentifizierung von einem der externen Geräte, die auf eine oder mehrere externe Schnittstellen des Schnittstellensteuerungsmoduls zugegriffen haben, um zu bestimmen, ob das externe Gerät ein lizenzierter externer Gerätetyp ist, und es wird keine Verbindung zwischen dem externen Gerät und dem geschützten Host hergestellt, bevor das angeschlossene externe Gerät die Sicherheitsauthentifizierung bestanden hat; und
ein interner Speicher, der verwendet wird, um Daten auszutauschen, die zwischen den Schnittstellen übertragen werden,
wobei
wenn eine der externen Schnittstellen des Schnittstellensteuerungsmoduls ein externes Gerät zugreift, das Schnittstellensteuerungsmodul das Systemsteuerungsmodul benachrichtigt, dass das Systemsteuerungsmodul eine Sicherheitsauthentifizierungsoperation an dem externen Gerät durchführt;
wenn ein externes Gerät vom Nicht-Speichertyp in die zweite externe Schnittstelle (UA2) eingesteckt wird, das Schnittstellensteuerungsmodul das Systemsteuerungsmodul über die Steuerleitung benachrichtigt, und das Systemsteuerungsmodul die Hardware-Steuerungslogik des Schnittstellensteuerungsmoduls steuert, um einen physischen Schaltkreis zwischen der zweiten externen Schnittstelle (UA2) und der zweiten Weiterleitungsschnittstelle (UB2) einzuschalten, sodass das externe Gerät vom Nicht-Speichertyp mit der USB-Schnittstelle des Systemsteuerungsmoduls verbunden ist, während dieser Zeit hält die Hardware-Steuerungslogik einen physischen Schaltkreis zwischen der zweiten externen Schnittstelle (UA2) und der zweiten internen Schnittstelle (UA4), die mit dem geschützten Host verbunden ist, in einem getrennten Zustand; wenn das externe Gerät die Sicherheitsauthentifizierung nicht besteht, dann wird das externe Gerät als ein nicht lizenzierter Zugangsgerät eingestuft, und ein Schaltkreis zwischen dem externen Gerät und dem geschützten Host wird in einem physisch getrennten Zustand gehalten; wenn das externe Gerät ein Nicht-Speichertyp externes Gerät ist und die Sicherheitsauthentifizierung besteht, dann wird das externe Gerät als ein lizenzierter Zugangsgerät bestimmt, und ein physischer Schaltkreis zwischen der zweiten externen Schnittstelle (UA2) und der zweiten internen Schnittstelle (UA4) des Schnittstellensteuerungsmoduls wird eingeschaltet, um den physischen Schaltkreis zwischen dem externen Gerät vom Nicht-Speichertyp und dem geschützten Host einzuschalten; und
wenn das externe Gerät ein Speichertyp externes Gerät ist und die Sicherheitsauthentifizierung besteht, dann greift die interne Speicherschnittstelle (UB3) auf den internen Speicher zu, der Verbindungszustand zwischen der ersten externen Schnittstelle (UA1) für den Zugriff auf ein externes Speichertyp-Gerät und der ersten Weiterleitungsschnittstelle (UB1) wird durch einen Schalter des Schnittstellensteuerungsmoduls eingeschaltet, der Verbindungszustand zwischen der ersten Weiterleitungsschnittstelle (UB1) und der internen Speicher-

schnittstelle (UB3) wird durch einen Schalter des Schnittstellensteuerungsmoduls eingeschaltet, und der Verbindungszustand zwischen der internen Speicherschnittstelle (UB3) der ersten internen Schnittstelle (UA3) des Schnittstellensteuerungsmoduls wird durch einen Schalter des Schnittstellensteuerungsmoduls eingeschaltet; und
das Schnittstellensteuerungsmodul überwacht in Echtzeit den Verbindungszustand der externen Schnittstelle, die vom externen Gerät zugegriffen wird, und trennt automatisch den physisch verbundenen Schaltkreis, wenn das externe Gerät, das als ein lizenzierter Zugangsgerät bestimmt wurde, von der externen Schnittstelle abgezogen wird.

2. Anschlussschutzvorrichtung vom externen Verbindungstyp nach Anspruch 1, wobei
wenn das externe Gerät erneut zugegriffen wird, nachdem es von der externen Schnittstelle getrennt wurde, das Systemsteuerungsmodul die Sicherheitsauthentifizierungsoperation am externen Gerät erneut durchführt.

3. Anschlussschutzvorrichtung vom externen Verbindungstyp nach Anspruch 1, wobei

das Schnittstellensteuerungsmodul in Echtzeit einen Verbindungszustand aller internen Schnittstellen überwacht, die mit der entsprechenden Schnittstelle des geschützten Hosts verbunden sind;
wenn der Verbindungszustand abnormal ist, wird die Trennung eines Schaltkreises zwischen dem Schnittstellensteuerungsmodul und dem geschützten Host automatisch ausgelöst.

4. Anschlussschutzvorrichtung vom externen Verbindungstyp nach Anspruch 3, wobei
wenn der Verbindungszustand abnormal ist, das automatische Auslösen der Trennung des Schaltkreises zwischen dem Schnittstellensteuerungsmodul und dem geschützten Host weiterhin umfasst:
das Erfassen einer Strom-/Spannungsänderung an einer der internen Schnittstellen über einen Überwachungsschaltkreis, das Feststellen, dass der Verbindungszustand abnormal ist, und das Auslösen eines Alarmsignalanzeigers.

5. Anschlussschutzvorrichtung vom externen Verbindungstyp nach Anspruch 4, wobei
nachdem die Trennung des Schaltkreises zwischen dem Schnittstellensteuerungsmodul und dem geschützten Host automatisch ausgelöst wurde, der Verbindungszustand von abnormal zu normal wiederhergestellt wird, und der Schaltkreis zwischen dem Schnittstellensteuerungsmodul und dem geschützten Host weiterhin in einem getrennten Zustand gehalten wird.

6. Anschlussschutzvorrichtung vom externen Verbindungstyp nach Anspruch 1, wobei
das Systemsteuerungsmodul auf der Basis einer voreingestellten Sicherheitsrichtlinie die Sicherheitsauthentifizierung des an die eine oder mehrere externe Schnittstellen auf dem Schnittstellensteuerungsmodul angeschlossenen externen Geräts steuert.

7. Anschlussschutzvorrichtung vom externen Verbindungstyp nach Anspruch 1, wobei
das Schnittstellensteuerungsmodul einen Strom- und Spannungsbegrenzungsschaltkreis umfasst, um zu verhindern, dass die Anschlussschutzvorrichtung beschädigt wird, wenn die externe Schnittstelle ein stark entladendes Gerät anschließt.

8. Anschlussschutzvorrichtung vom externen Verbindungstyp nach Anspruch 1, wobei
eine oder mehrere der internen Schnittstellen und der externen Schnittstellen USB-Schnittstellen sind.

9. Schutzsystem, umfassend:

ein oder mehrere externe Geräte,
einen geschützten Host, und
die Anschlussschutzvorrichtung vom externen Verbindungstyp wie in einem der Ansprüche 1-8 beansprucht, wobei
die Anschlussschutzvorrichtung vom externen Verbindungstyp extern mit dem geschützten Host verbunden ist, so dass die ein oder mehreren externen Geräte eine Schnittstellenkommunikation mit dem geschützten Host über die Anschlussschutzvorrichtung vom externen Verbindungstyp durchführen.

Revendications

1. Dispositif de protection de terminal externe, comprenant:

un module de contrôle d'interface, utilisé pour fournir une première interface externe (UA1), une deuxième interface externe (UA2), une première interface de transfert (UB1), une deuxième interface de transfert (UB2), une interface de stockage interne (UB3), une première interface interne (UA3) et une deuxième interface interne (UA4), la première interface interne (UA3) et la interface deuxième interne (UA4) étant connectées aux interfaces correspondantes d'un hôte protégé, la première interface externe (UA1) étant configurée pour être accédée

par un dispositif externe de type stockage, et la deuxième interface externe (UA2) étant configurée pour être accédée par un dispositif externe de type non-stockage;

un module de contrôle système, comprenant une interface USB, la première interface de transfert (UB1) et la deuxième interface de transfert (UB2) accédant à l'interface USB, en outre, le module de contrôle système étant connecté au module de contrôle d'interface via une ligne de contrôle, et contrôlant l'authentification de sécurité de tout dispositif externe accédé aux une ou plusieurs interfaces externes sur le module de contrôle d'interface, afin de déterminer si le dispositif externe est un dispositif externe autorisé, et aucune connexion n'étant fournie entre le dispositif externe et l'hôte protégé avant que le dispositif externe branché ne passe l'authentification de sécurité; et

une mémoire interne utilisée pour stocker des données échangées entre les interfaces,

où

lorsqu'une des interfaces externes du module de contrôle d'interface accède à un dispositif externe, le module de contrôle d'interface informe le module de contrôle système que le module de contrôle système effectue une opération d'authentification de sécurité sur le dispositif externe;

lorsqu'un dispositif externe de type non-stockage est branché dans la deuxième interface externe (UA2), le module de contrôle d'interface informe le module de contrôle système via la ligne de contrôle, et le module de contrôle système contrôle la logique de contrôle matériel du module de contrôle d'interface pour activer un circuit physique entre la deuxième interface externe (UA2) et la deuxième interface de transfert (UB2), de sorte que le dispositif externe de type non-stockage soit connecté à l'interface USB du module de contrôle système, pendant ce temps, la logique de contrôle matériel maintient un circuit physique entre la deuxième interface externe (UA2) et la deuxième interface interne (UA4) connectée à l'hôte protégé dans un état déconnecté; si le dispositif externe ne passe pas l'authentification de sécurité, alors le dispositif externe est défini comme un dispositif d'accès non autorisé, et un circuit entre le dispositif externe et l'hôte protégé est maintenu dans un état physiquement déconnecté ; si le dispositif externe est un dispositif externe de type non-stockage et passe l'authentification de sécurité, alors le dispositif externe est déterminé comme un dispositif d'accès autorisé, et un circuit physique entre la deuxième interface externe (UA2) et la deuxième interface interne (UA4) du module de contrôle d'interface est activé, afin d'activer le circuit physique entre le dispositif externe de type non-stockage et l'hôte protégé; et

si le dispositif externe est un dispositif externe de type stockage et passe l'authentification de sécurité, alors l'interface de stockage interne (UB3) accède à la mémoire interne, l'état de connexion entre la première interface externe (UA1) pour accéder à un dispositif externe de type stockage et la première interface de transfert (UB1) sont activés par un commutateur du module de contrôle d'interface, l'état de connexion entre la première interface de transfert (UB1) et l'interface de stockage interne (UB3) sont activés par un commutateur du module de contrôle d'interface, et l'état de connexion entre l'interface de stockage interne (UB3) de la première interface interne (UA3) du module de contrôle d'interface sont activés par un commutateur du module de contrôle d'interface; et

le module de contrôle d'interface surveille en temps réel un état de connexion de l'interface externe accédée par le dispositif externe, et déconnecte automatiquement le circuit physiquement connecté lorsque le dispositif externe déterminé comme un dispositif d'accès autorisé est débranché de l'interface externe.

2. Dispositif de protection de terminal externe selon la revendication 1, dans lequel

lorsque le dispositif externe est reconnecté après avoir été débranché de l'interface externe, le module de contrôle système réexécute l'opération d'authentification de sécurité sur le dispositif externe.

3. Dispositif de protection de terminal externe selon la revendication 1, dans lequel

le module de contrôle d'interface surveille en temps réel l'état de connexion de toutes les interfaces internes connectées à l'interface correspondante de l'hôte protégé;

lorsque l'état de connexion est anormal, la déconnexion d'un circuit entre le module de contrôle d'interface et l'hôte protégé est automatiquement déclenchée.

4. Dispositif de protection de terminal externe selon la revendication 3, dans lequel

lorsque l'état de connexion est anormal, le déclenchement automatique de la déconnexion du circuit entre le module de contrôle d'interface et l'hôte protégé comprend en outre:

la capture d'un changement de courant/tension de l'une quelconque des interfaces internes via un circuit de surveillance, la détermination que l'état de connexion est anormal, et le déclenchement d'un signal d'indication d'alarme.

5. Dispositif de protection de terminal externe selon la revendication 4, dans lequel
après que la déconnexion du circuit entre le module de contrôle d'interface et l'hôte protégé ait été automatiquement déclenchée, l'état de connexion se restaure de l'anormalité à la normalité, et le circuit entre le module de contrôle d'interface et l'hôte protégé est maintenu dans un état déconnecté.

6. Dispositif de protection de terminal externe selon la revendication 1, dans lequel
le module de contrôle système contrôle, sur la base d'une politique de sécurité prédéfinie, l'authentification de sécurité du dispositif externe accédant à une ou plusieurs interfaces externes sur le module de contrôle d'interface.

7. Dispositif de protection de terminal externe selon la revendication 1, dans lequel
le module de contrôle d'interface comprend un circuit limité en courant et en tension pour empêcher le dispositif de protection de terminal externe d'être endommagé lorsque l'interface externe accède à un dispositif à décharge forte.

8. Dispositif de protection de terminal externe selon la revendication 1, dans lequel
une ou plusieurs des interfaces internes et des interfaces externes sont des interfaces USB.

9. Système de protection, comprenant:

un ou plusieurs dispositifs externes,
un hôte protégé, et
le dispositif de protection de terminal externe tel que revendiqué dans l'une quelconque des revendications 1 à 8, dans lequel
le dispositif de protection de terminal externe est connecté extérieurement à l'hôte protégé, de sorte que le ou les dispositifs externes effectuent une communication d'interface avec l'hôte protégé via le dispositif de protection de terminal externe.

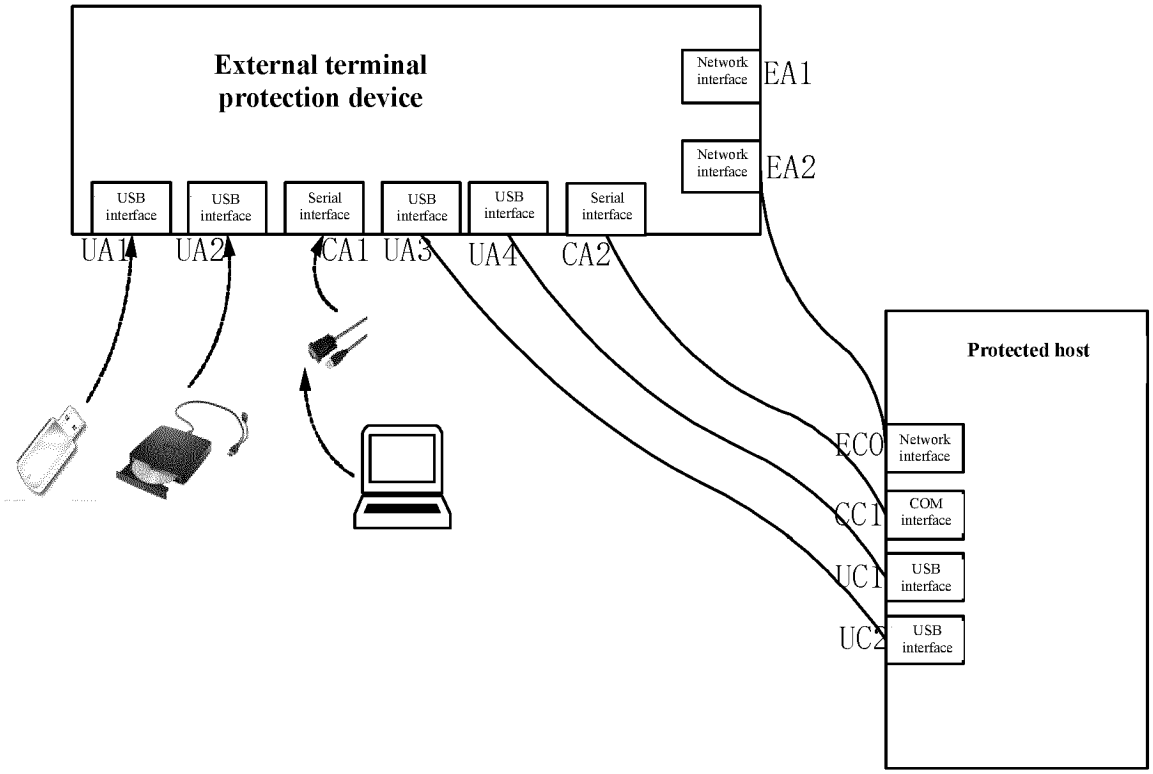
External terminal protection device
Network interface
EA1
Network interface
EA2
USB interface
USB interface
Serial interface
USB interface
USB interface
Serial interface
UA1
UA2
CA1
UA3
UA4
CA2
Protected host
EC0
Network interface
CC1
COM interface
UC1
USB interface
UC2
USB interface

Fig. 1

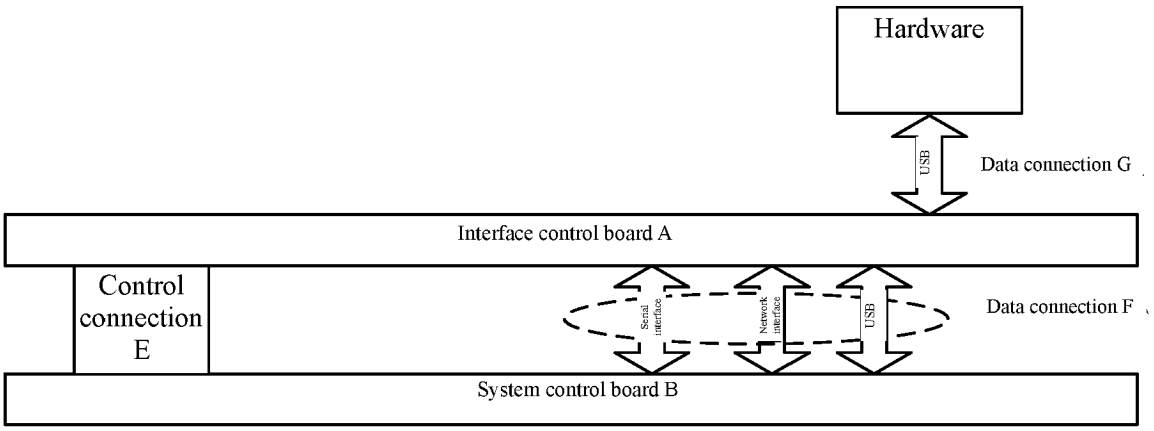
Hardware
USB
Data connection G
Interface control board A
Control connection E
Serial interface
Network interface
USB
Data connection F
System control board B

Fig. 2

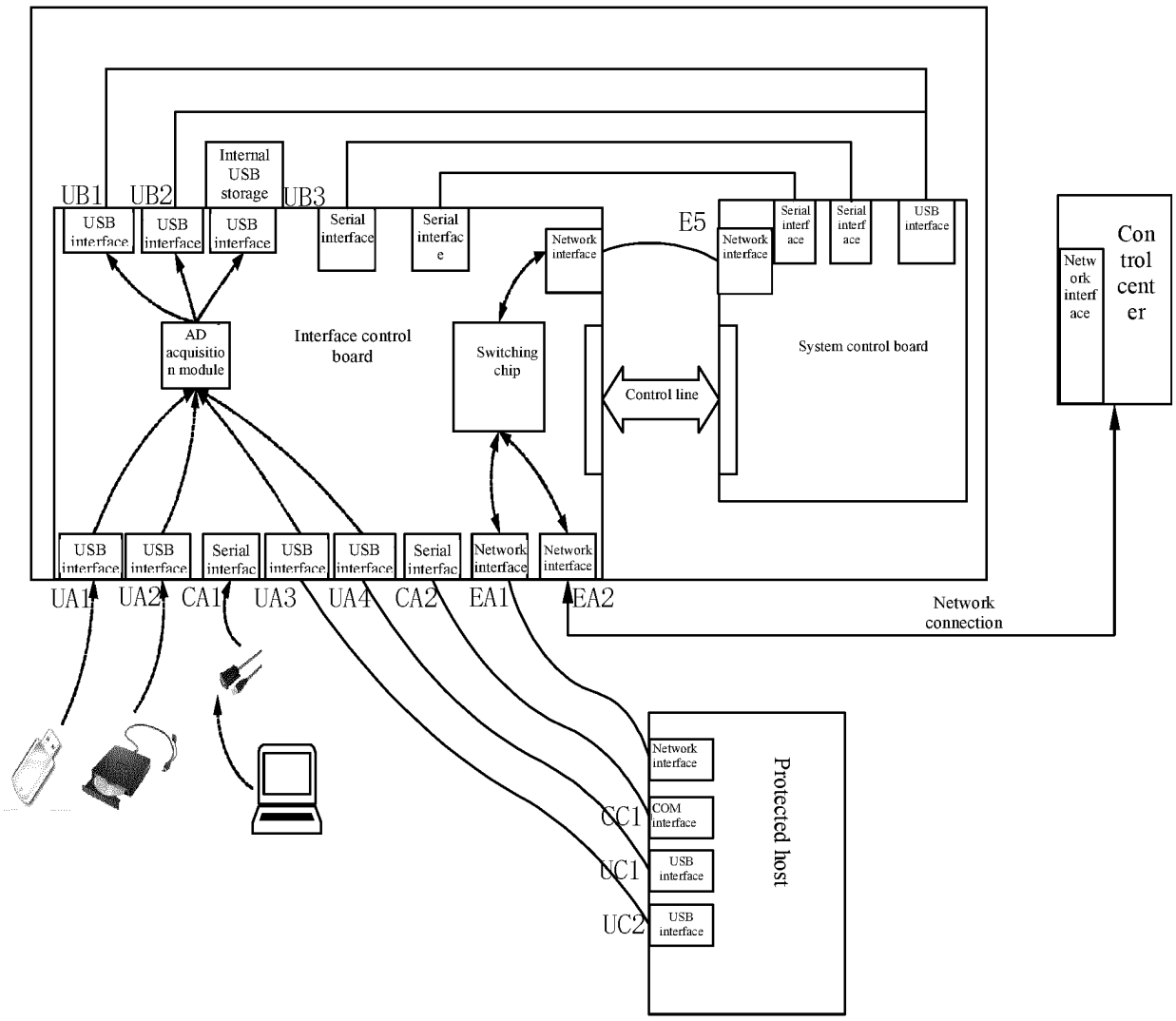
Internal USB storage
UB1
UB2
UB3
USB interface
USB interface
USB interface
Serial interface
Serial interfac e
Network interface
E5
Network interface
Serial interf ace
Serial interf ace
USB interface
AD acquisitio n module
Interface control board
Switching chip
Control line
System control board
Netw ork interf ace
Con trol cent er
USB interface
USB interface
Serial interfac
USB interface
USB interface
Serial interfac
Network interface
Network interface
UA1
UA2
CA1
UA3
UA4
CA2
EA1
EA2
Network connection
Network interface
COM interface
USB interface
USB interface
CC1
UC1
UC2
Protected host

Fig. 3

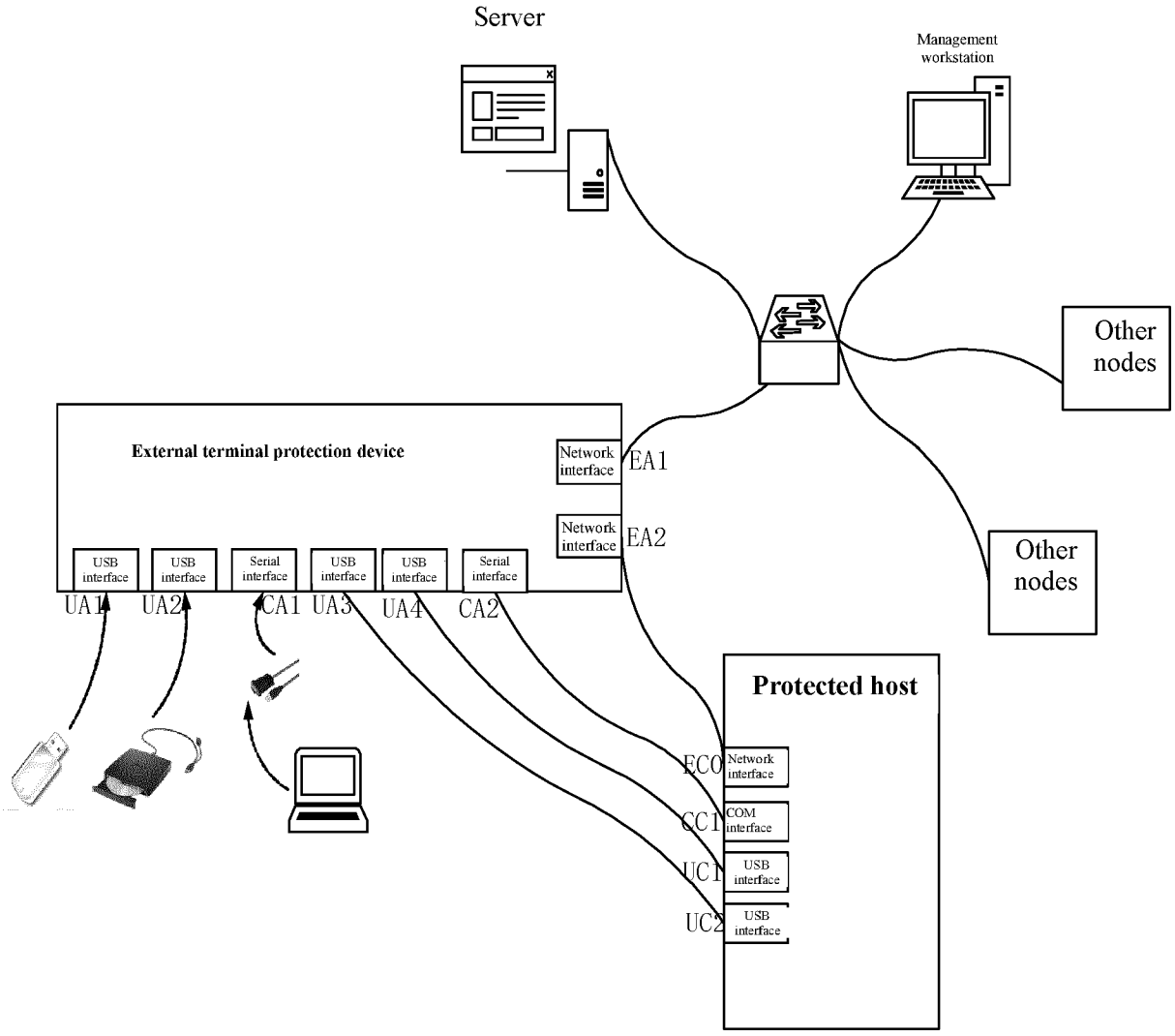
Server
Management workstation
Other nodes
External terminal protection device
Network interface
EA1
Network interface
EA2
USB interface
USB interface
Serial interface
USB interface
USB interface
Serial interface
UA1
UA2
CA1
UA3
UA4
CA2
Other nodes
Protected host
EC0
Network interface
CC1
COM interface
UC1
USB interface
UC2
USB interface

Fig. 4

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 2015365237 A1 **[0005]**
- US 7877788 B1 **[0006]**
- US 20180137278 A1 **[0007]**
- FR 2949888 A1 **[0008]**